**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

Docket No.: BARTH-2

| | |
|---|---|
| **In re PATENT Application of:** | ) |
| **RAINER BARTH** | ) **Examiner: Jerry B. Dennison** |
| | ) **Group Art Unit: 2443** |
| **Appl. No.: 10/659,766** | ) |
| **Filed: September 10, 2003** | ) |
| | ) **Confirmation No.: 4858** |
| **For: METHOD FOR TRANSMITTING MESSAGES OF INDUSTRIAL CONTROLLERS TO PRE-DEFINED RECEIVERS VIA THE INTERNET** | ) |

# BRIEF OF APPEAL

**CERTIFICATION OF EFS-WEB TRANSMISSION**

I hereby certify that this paper is being EFS-Web transmitted to the U.S. Patent and Trademark Office, Alexandria VA 22313-1450, on **September 23, 2011.**
Date

Henry M. Feiereisen
(Name of Registered Representative)

(Signature) 9-23-2011 (Date of Signature)

Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

S I R:

This is an appeal from the final rejection of claims 1-12, 14, 15 and 17-26 by the Primary Examiner. The Brief is being filed under the provisions of 37 C.F.R. §41.37. The amount of $540.00 to cover the requisite fee set forth in 37 C.F.R. §41.20(b)(2) is being paid by credit card.

To the extent necessary, a petition for an extension of time under 37 C.F.R. §1.136 is hereby made. Accompanying this Brief of Appeal is the appropriate fee of $130.00 for a one month extension.

The Commissioner is hereby authorized to charge fees which may be required, or credit any overpayment to Deposit Account No. 06-0502.

## (1) REAL PARTY IN INTEREST

The above-referenced patent application has been assigned to Siemens Aktiengesellschaft, having a place of business at Wittelsbacherplatz 2, 80333 München, Germany, the real party in interest by virtue of an assignment recorded on 12/24/2003 at reel 014844, frame 0903.

## (2) RELATED APPEALS AND INTERFERENCES

There are no and there have been no related appeals or interferences that will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

## (3) STATUS OF CLAIMS

The following claims are in the appeal proceedings:

Claims 1-4, 7-12, 14-15 and 17-26 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie et al. (US 7203560) in view of Zhou et al. (US 20080186166). Claims 13 and 16 have been cancelled.

Claim 5 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie et al. (US 7203560) in view of Zhou et al. (US 20080186166) further in view of Qi et al. (US6892064).

Claim 6 stands rejected under 35 U.S.C. §103(a) as being unpatentable over Wylie et al. (US 7203560) in view of Zhou et al. (US 20080186166) further in view of Subramaniam et al. (US20070208697).

## (4) STATUS OF AMENDMENTS

Appellant has filed Request for a Panel Review together with the Notice of Appeal. The Notice of Panel Decision states that claims 1-12, 14, 15, 17-26 are rejected.

## (5) SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 recites a method for securely providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network. A specific receiver is assigned to each specific industrial control alarm event occurring in the machine and event-relevant information including sensitive information is written to a database in the controller controlling the machine. A receiver-specific message indicating that an alarm event has occurred and not containing said sensitive information is transmitted from the controller to the specified receiver in response to an alarm event.

Independent claim 1 accesses the sensitive information and other event-relevant information via a Web server using a cryptographically protected communication protocol based on an Internet browser in response to the receiver-specific message from the controller. At least one of failure analysis or fault repair is performed on the machine using sensitive information accessed using said cryptographically protected communication protocol.

Independent claim 11 accesses the sensitive information and other event-relevant information using a modem connection protected by an authentication protocol in response to the receiver-specific message from the controller. At least one of failure analysis or fault repair is performed on the machine using sensitive information accessed using said protected modem connection.

In paragraph [0006], the specification explains that the communications and security problem addressed by the invention is the result of reliance on highly-

automated industrial plants. The potential costs and liabilities associated with unauthorized access to the information used by machine controllers are increasing as manufacturing plants become increasingly more highly automated.

## (6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Issue 1- Whether a hindsight argument that addresses a lack of motivation in a cited disclosure and related art to combine that disclosure with a second unrelated disclosure, is "spurious" because it does not distinguish the limitations of the claim from the cited prior art.

Issue 2- Whether claims 1 and 11, and the claims dependent thereon, are obvious over Wylie et al. (US 7203560) in view of Zhou et al. (US 20080186166).

## (7) ARGUMENT

Issue 1- Whether a hindsight argument that addresses a lack of motivation in a cited disclosure to combine that disclosure with a second unrelated disclosure, is "spurious" because it does not distinguish the limitations of a claim from the cited prior art.

In the final Office Action, the Examiner responded to applicant's arguments by saying "Applicant does not present any substantive arguments to distinguish the limitations of the claim from the cited prior art." However, applicant's position is and has been that the Examiner's obviousness rejection is and has been based on hindsight.

The Examiner's "Response to Arguments" suggests that any such argument as hindsight, which addresses invalidly combined disclosures rather than just being "specific to the claimed limitations" of applicant's claims, is to be ignored as spurious. This is erroneous.

There must be motivation in Wylie's automated industrial machine controllers to combine them with Zhou's inappropriate, centralized multi-purpose public service

bureau. There is none. There can be none because applicant's communication is from the controller to the recipient of the alarm message, not to some centralized office. No attempt has been made to provide either 1) motivation, or 2) a more plausibly suitable second reference. The invention is not obvious if this communications problem can't be solved without relying on hindsight, i.e., without copying applicant's disclosed invention. Wylie doesn't disclose the problem. Zhou isn't a solution.

Issue 2- Whether claims 1 and 11, and the claims dependent thereon, are obvious over Wylie et al. (US 7203560) in view of Zhou et al. (US 20080186166).

The Wylie patent discloses conventional industrial controllers. However, Wylie also suggests that there is no problem with the conventional communications methods they use, disclosing the use of Internet email as well as other public and private wireless and hardwired communications networks, without regard for the well-known security vulnerabilities of the public networks, and the very limited geographic accessibility of private and hard-wired systems, see col. 5, lines 60-65, and col. 8, lines 30-53. Applicant has found that

Neither Wylie, nor the German disclosures of industrial controllers that are of record in this application, which also use conventional communications methods, describes or suggests the lack of secure, timely information encountered by Germany's roving technicians who constantly travel from one automated plant to another. Technicians need to receive alarm event messages in real time over whatever public networks they can access from wherever they happen to be. They can't rely on private networks, much less on their central office or Zhou's central service bureau. When a problem isn't yet recognized, there logically can be no "obvious" solution.

Zhou even teaches away from applicant's advantageous de-centralized alarm communications system. Zhou's remote ASP services bureau is advantageous, and potentially profitable, because it provides many monitoring and alarm functions for many different events that occur in many different places, all from at the same one

centralized location-- see Zhou, paragraph **[0005]**. Thus, Zhou's alarms are all from Zhou's central office.

In contrast the travelling technician needs immediate access to a particular controller in order to assure continued safe operation of that controller, not just to some central office. The conventional security measures such as PKI, that are used by controllers to email or otherwise contact a central office in the disclosures of record in this application, are not usable to contact these roving technicians. See paragraph [0007] of the application.

Thus, applicant's system is entirely de-centralized. Each controller even designates the specific receiver of its alarm message. See paragraph [0024]. Thus, it is that this "alarm message" is recited in claims 1 and 11 as being "from the controller" unlike Zhou's alarms.

For the reasons set forth above, it is respectfully requested that the rejection of claims 1 and 11 and the claims dependent thereon under 35 U.S.C. 103(a) be reversed.

Respectfully submitted,

By: _____
Henry M. Feiereisen
Agent for Appelant
Reg. No.: 31,084

Date: September 23, 2011
708 Third Avenue
Suite 1501
New York, N.Y. 10017
(212) 244-5500
HMF/RL:be

## (8) CLAIMS APPENDIX

1. A method for securely providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network, comprising the steps of:

assigning a specific receiver to each specific industrial control alarm event occurring in the machine;

writing event-relevant information to a database in the controller controlling the machine, said event-relevant information including sensitive information;

transmitting from the controller to the specified receiver in response to the alarm event a receiver-specific message indicating that the alarm event has occurred and not containing said sensitive information;

accessing the event-relevant information via a Web server using a cryptographically protected communication protocol based on an Internet browser in response to the receiver-specific message; and

performing at least one of failure analysis or fault repair on the machine using sensitive information accessed using said cryptographically protected communication protocol.

2. The method of claim 1, wherein the cryptographically protected communication protocol based on the Internet browser comprises a "Hypertext Transfer Protocol Security" protocol.

3. The method of claim 2, wherein the "Hypertext Transfer Protocol Security" protocol comprises a "Secure Socket Layer" protocol or a "Transport Layer Security" protocol.

4. The method of claim 1, wherein the receiver-specific message is transmitted to the specified receiver as an e-mail message, an SMS message or a voice message.

5. The method of claim 4, wherein the e-mail message includes a cross-reference, in particular a URL address, that provides a link to the event-relevant information that is stored in the database for the specified receiver.

6. The method of claim 1, wherein the event-relevant information written to the database for the specified receiver includes file attachments which are stored in the database for the specified receiver.

7. The method of claim 1, wherein access to the Web server is protected by a login prompt and a password.

8. The method of claim 1, wherein the Web server is integrated with hardware of the controller.

9. The method of claim 1, wherein at least one of the database and the Web server are implemented as hardware that is separate from hardware of the controller.

10. The method of claim 1, further comprising the step of transmitting at least one of data, parameters and programs from the specified receiver to the controller.

11. A method for securely providing event-relevant information about an industrial control alarm event occurring in a machine from an industrial controller controlling the machine to a specified remote receiver via a network, comprising the steps of:

assigning a specific receiver to each specific industrial control alarm event

occurring in the machine;

writing event-relevant information to a database in the controller controlling the machine, said event-relevant information including sensitive information;

transmitting from the controller to the specified receiver in response to the alarm event a receiver-specific message indicating that the alarm event has occurred and not containing said sensitive information;

accessing the event-relevant information using a modem connection protected by an authentication protocol in response to the receiver-specific message; and

performing at least one of failure analysis or fault repair on the machine using sensitive information accessed using said protected modem connection.

12. The method of claim 1, wherein the event-relevant information written to the data base includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

13. (Cancelled)

14. The method of claim 1, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

15. The method of claim 11, wherein the event-relevant information written to the data base includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

16. (Cancelled)

17. The method of claim 11, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

18. The method of claim 11, further comprising the step of transmitting at least one of data, parameters and programs from the specified receiver to the controller.

19. The method of claim 11, wherein the event-relevant information that is written to the database includes at least one of event messages, fault messages, information about machine status and process information, or a combination thereof.

20. The method of claim 1, wherein only a receiver-specific message indicating that a specified alarm event has occurred is transmitted to the specified receiver.

21. The method of claim 1 wherein the event-relevant information is written to a receiver-specific database element of the database.

22. The method of claim 11 wherein the event-relevant information is written to a receiver-specific database element of the database.

23. The method of claim 1 wherein event-relevant information written to the database for the specified receiver is accessed in response to the receiver-specific message.

24. The method of claim 11 wherein event-relevant information written to the database for the specified receiver is accessed in response to the receiver-specific message.

25. The method of claim 1 wherein said fault repair is performed by uploading information to the controller using said cryptographically protected communication protocol.

26. The method of claim 11 wherein said fault repair is performed by uploading information to the controller using said protected modem connection.

## (9) EVIDENCE APPENDIX

NONE

## (10) RELATED PROCEEDINGS APPENDIX

NONE